UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/710,987	11/08/2000	Richard Schroeppel	2944.2.1	5823

28049 7590 04/22/2004

PATE PIERCE & BAIRD
215 SOUTH STATE STREET, SUITE 550
PARKSIDE TOWER
SALT LAKE CITY, UT 84111

EXAMINER	
DADA, BEEMNET W	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 04/22/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/710,987	SCHROEPPEL, RICHARD	
	Examiner	Art Unit	
	Beemnet W Dada	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 November 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-59* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-59* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *2 & 5*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-59 have been examined.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claim 1-5, 8, 13-16, 26-28, 30, 33, 35-37, 42-45, 48-52 and 56-58 are rejected under 35 U.S.C. 102(e) as being anticipated by Vanstone et al. (hereinafter refereed to as Vanstone) (U.S. Patent No. 6,141,420).

4. As per claim 1, Vanstone teaches a method comprising:

selecting an elliptic curve method [column 2, lines 60-63];

executing a point modification algorithm to manipulate points of the elliptic curve method [column 2, lines 35-43];

generating a signal having a distinct characteristic (i.e. generating an encryption key) using the selected elliptic curve method [column 2, lines 65-67 & column 3, lines 1-11];

providing substantive content (i.e. sending / receiving a message) [column 2, lines 60-63]; and

manipulating the substantive content (i.e. encrypting/decrypting) using the distinct characteristic [column 3, lines 12-13].

5. As per claims 26 and 29, Vanstone teaches an apparatus comprising:

a system for creating a distinct characteristic configured to support cryptographic manipulation of information [column 8, lines 20-25];

a memory device operably connected to the system for storing the distinct characteristic and executables programmed to operate on the distinct characteristic [column 8, lines 55-60];

an encrypting device operably connected to the system for controlling an encryption process using the distinct characteristic [column 8, lines 60-67];

the system further configured to execute an elliptic curve method for generating the distinct characteristic [column 2, lines 60-63]; and

the system further configured to execute a point modification algorithm for generating the distinct characteristic [column 2, lines 35-43].

6. As per claims 2, 27, and 30, Vanstone teaches the method/apparatus as applied to claims 1, 26 and 30 above. Furthermore Vanstone teaches the method/apparatus, wherein the point modification algorithm is selected from point addition, point subtraction, point fractioning, point multiplying, rotating, negative point modification, and a combination of one or more thereof [column 4, lines 55-57, column 3, lines 56-64, column 10, line 61].

7. As per claims 3 and 4, Vanstone teaches the method as applied to claim 1 above. Furthermore, Vanstone teaches the method, wherein manipulating the substantive content comprises encrypting / decrypting the substantive content [column 3, lines 12-13 and column 3, lines 19-20].

8. As per claims 8, and 33, Vanstone teaches the method/apparatus as applied to claims 1 and 29 above. Furthermore, Vanstone teaches the method further comprising dynamically specifying the point modification algorithm in lieu of specifying the modification operation in advance (generating a session key randomly during a session) [column 3, lines 1-15].

9. As per claim 13, Vanstone teaches the method as applied to claim 2 above. Furthermore, Vanstone teaches the method, further comprising selecting a first point and pre-modifying (in a predetermined method) the first point by a modification operation configured to compensate for some of the processing steps, added and

corresponding to execution of a series of steps in accordance with the method [column 5, lines 56-67].

10. As per claim 14, Vanstone teaches the method as applied to claim 1 above. Furthermore, Vansotne teaches the method, further comprising sending by a sender and receiving by a receiver the substantive content, and wherein the sender executes a first operation during modification for encryption and the receiver executes a sedond and distinct operation during modification for decryption [column 2, lines 60-67 and column 3, lines 1-24].

11. As per claims 5, 15 and 35, Vanstone teaches the method/apparatus as applied to claim 1 and 29 above. Furthermore, Vanstone teaches the method, wherein generating the distinct characteristic further comprises creating a distinct characteristic selected from a symmetric key configured to be shared by two or more parties, a decryption code for processing an encrypted signal, a digital signature, an asymmetric key, and an authentication (i.e. public/private keys used for encryption/decryption, authentication and a shared session key used for encryption/decryption) [column 3, 1-24].

12. As per claim 16, Vanstone teaches the method as applied to claim 1 above. Furthermore, Vanstone teaches the method, further comprising selecting a point and

wherein the point is of a type selected from a hyperelliptic curve, an algebraic curve, and abelian variety [column 3, lines 49-56].

13. As per claim 28, Vanstone teaches the apparatus as applied to claim 26 above. Furthermore, Vanstone teaches the apparatus, wherein the distinct characteristic is configured to be processable by the system for divulging independently to two independent parties a secret to be shared by the two independent parties [column 3, lines 9-15].

14. As per claim 36, Vanstone teaches the method as applied to claim 1 above. Furthermore, Vanstone teaches the method, wherein the elliptic curve is over a finite field [column 2, lines 27-32]; the finite field is represented by a field polynomial [column 2, lines 29-30]; and the field polynomial is of low hamming weight [column 13, lines 60-62].

15. As per claim 37, Vanstone teaches the method as applied to claim 36 above. Furthermore, Vanstone teaches the method, wherein the field polynomial is selected form a binomial, a trinomial, and a pentanomial (i.e. polynomials of degree 2, 3, and 5) [column 8, lines 39-41, and column 6, lines 30-32].

16. As per claim 42, and 53-55, Vanstone teaches the method as applied to claim 1 above. Furthermore, Vanstone teaches the method, wherein the point modification

algorithm comprises solving a quadratic equation using efficient algorithm [column 20, claim 32, and column 21, claims 39 & 40].

17. As per claim 43, Vanstone teaches the method as applied to claim 1 above. Furthermore, Vanstone teaches the method, wherein the point modification algorithm comprises computing a reciprocal (multiplicative inverse) of a field element using efficient algorithm [column 11, lines 39-42].

18. As per claim 44, Vanstone teaches the method as applied to claim 1 above. Furthermore, Vanstone teaches the method, wherein the point modification algorithm comprises at least one of adding and subtracting of elliptic curve points using efficient algorithm [column 12, lines 35-41].

19. As per claim 45, Vanstone teaches the method as applied to claim 44 above. Furthermore, Vanstone teaches the method wherein the addition and subtraction comprises computing a reciprocal of a field element using an efficient algorithm [column 15, lines 56-67 and column 16, lines 1-16].

20. As per claim 49, Vanstone teaches the method as applied to claim 1 above. Furthermore, Vanstone teaches the method, wherein the point modification algorithm further comprises choosing a multiplier having a low hamming weight [column 13, lines 60-62].

21. As per claim 50, Vanstone teaches the method as applied to claim 1 above. Furthermore, Vanstone teaches the method, wherein the point modification algorithm includes point addition and subtraction steps and the point modification algorithm is chosen to minimize the number of steps [column 3, lines 56-62 and column 4, lines 49-65].

22. As per claims 47, 48 and 51, Vanstone teaches the method as applied to claim 1 above. Furthermore, Vanstone teaches the method, wherein the point modification algorithm is an addition-subtraction chain intermixed with point fractioning [column 4, lines 7-25].

23. As per claim 52, Vanstone teaches the method as applied to claim 1 above. Furthermore, Vanstone teaches the method, wherein the elliptic curve is over a finite field, and the size of the finite field is increased such that a smaller number of addition and subtraction steps may be combined with a larger number of point fractioning steps, such that the overall computation effort is reduced, while preserving a specified level of security [column 4, lines 7-63].

24. As per claims 56-58, Vanstone teaches the method as applied to claim 1 above. Furthermore, Vanstone teaches the method, wherein the modification algorithm further comprises:

Using plurality of representations of the points, using input points in one or more representations to produce output points in a different representation wherein at least three changes of representation occur [column 15, lines 51-65 and column 16, lines 1-20].

Claim Rejections - 35 USC § 103

25. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

26. Claims 6, 7, 9-12, 17-25, 31, 32 and 59 are rejected under 35 U.S.C. 103(a) as being unpatentable over Vanstone et al. (U.S. Patent No. 6,141,420).

27. As per claims 6, 7, 21, 31 and 32, Vanstone teaches the method/apparatus as applied to claims 1, 2, 27, and 30 above. Furthermore, Vanstone teaches executing modification algorithm to manipulate points of the elliptic curve method [column 2, lines 35-43]. Vanstone also teaches modification algorithms selected form point multiplying, point fractioning [column 4, lines 55-57, column 3, lines 56-64, column 10, line 61]. However, Vanstone does not explicitly teach integral, imaginary and complex methods used for point multiplying and point fractioning. It would have been obvious to a person

skilled in the art at the time the invention was made to include integral, imaginary and complex methods into point multiplying, and point fractioning methods thought by Vanstone so that the point multiplication and point fractioning would be selected from those methods.

28. As per claims 9, 10 and 34, Vanstone teaches the method/apparatus as applied to claims 2 and 30 above. Furthermore, Vanstone teaches the method/apparatus further comprising selecting a first point for execution of the point modification algorithm, based on a selected property [column 2, lines 27-31 and lines 39-43].

29. As per claims 11 and 12, Vanstone teaches the method as applied to claim 10 above. Furthermore, Vanstone teaches the method further comprising repeating the point modification algorithm with second point selected by another entity selected from deterministic process, a random process, and a third party [column 3, lines 17-23]; wherein the second point is communicated to the point modification in a format from a message and certificate [column 3, lines 14-15].

30. As per claims 17-20, 22-25, and 46 Vanstone teaches the method as applied to claim 1 above. Furthermore, Vanstone teaches point represented in Cartesian space and point existing in a mapped Cartesian space having Cartesian representation (i.e. a point P represented as P(x,y) (x coordinate, y coordinate) [column 2, lines 60-62]. Vanstone also teaches point multiplication in a finite group whose member lie on an

elliptic curve [column 2, lines 27-30 and column 4, lines 55-58]. However, Vanstone does not explicitly teach multiplication per halving operation. It is well known to have multiplication per halving operation in a method of arithmetic multiplication. Therefore, It would have been obvious to one having ordinary skill in the art at the time the invention was made to implement multiplication per halving operation so that the multiplication thought by Vanstone would be performed by halving operation.

31. Claims 38-41 are rejected under 35 U.S.C 103(a) as being unpatentable over Vanstone et al. (U.S. Patent No. 6,141,420) in view of Elkies (Ref V).

32. As per claim 38, Vanstone teaches the method as applied to claim 1 above. Furthermore, Vansotne teaches the elliptic curve wherein the finite field is represented by a polynomial [column 2, lines 29-30]. However, Vanstone does not explicitly teach the finite field represented as a field tower. Elkies teaches a finite field represented as a field tower [page 1, paragraphs 1&2]. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to implement a finite field represented as a field tower thought by Elkies into the finite field represented by field polynomial thought by Vanstone, in order to easily calculate genus of a curve in a tower.

33. As per claim 39, the combination of Vanstone and Elkies teaches the method as applied to claim 38 above. Furthermore, Elkies teaches the method, wherein the field

tower comprises an outer field, and the extension degree of the outer field is selected from the numbers 2, 3, 5, a product of the numbers, or repeated uses of the numbers [page 3, paragraph 2 ff].

34. As per claim 40, the combination of Vanstone and Elkies teaches the method as applied to claim 38 above. Furthermore, Elkies teaches the method, wherein the field tower has more than two levels [page 1,paragraph 2].

35. As per claim 41, the combination of Vanstone and Elkies teaches the method as applied to claim 38 above. Furthermore, Elkies teaches the method, wherein the field tower comprises an inner field, having arithmetic, and wherein the arithmetic is accelerated by using pre-computed tables for operations selected from the group consisting of multiplication, squaring, taking the square root, division, reciprocation, taking the logarithm, exponentiation, calculating solutions of quadratic equations, and calculating the solution of polynomial equations [page 3, paragraph 2 ff].

36. As per claim 59, the claimed steps correspond to the functions of the elements of the method claim 18, which has been rejected above and thus rejected with the same reason applied thereto.

Conclusion

37. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a) U.S. Patent No. 6,337,909 B1 to Vanstone et al.

b) U.S. Patent No. 6,480,606 B1 to Kurumatani.

c) U.S. Patent No. 6,263,081 B1 to Miyaji et al.

d) U.S. Patent No. 5,854,759 to Kaliski, Jr. et al.

e) U.S. Patent No. 6,212,277 B1 to Miyaji.

f) Elliptic Scalar Multiplication Using Point Halving, to Erik Knudsen.

g) On computing a multiple of an elliptic curve to Lopez et al.

h) Efficient Finite Field Basis conversion Involving Dual Bases to Kaliski et al.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Beemnet W Dada whose telephone number is (703) 305-8895. The examiner can normally be reached on Monday - Friday (8:30 am - 6:00 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y Vu can be reached on (703) 305-4393. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Beemnet Dada

April 7, 2004